



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

July 1, 2019

VIA E-MAIL: 74887-37730402@requests.muckrock.com

Emma Best
c/o MuckRock News
DEPT MR 74887
411A Highland Avenue
Somerville, Massachusetts 02144

Dear Ms. Best:

This is in response to your Freedom of Information Act (FOIA) request, dated and received on June 5, 2019, seeking access to records maintained by the Treasury Inspector General for Tax Administration (TIGTA).

Specifically, you have requested the following records (directly from your request):

Copies of records mentioning or describing audits, reviews, investigations or reports regarding the agency's cyber security, including audits or investigations regarding the state of the agency's cyber security regarding potential attacks as well as audits and investigations conducted in the wake of a suspected or actual cyber attack, hacking incident or breach. Please include materials generated between 1 January 1996 and 30 June 2016.

TIGTA was established under the IRS Restructuring and Reform Act of 1998 and stood up as a Treasury Bureau on January 1, 1999. Therefore, the period of our search for responsive records was January 1, 1999 through June 30, 2016.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

We have considered your request as consisting of two parts. In the first part, we have construed your request as seeking records that review TIGTA's cybersecurity program. TIGTA's Office of Information Technology, Cybersecurity Security Services, conducted a search of its records and located two (2) internal cybersecurity assessment reports as being responsive to your request.

A report titled *Evaluation of TIGTA Enterprise System (TES) Controls*, dated June 9, 2015, consists of twenty (20) pages. We are releasing to you one (1) page in full and two (2) pages in part. A copy is enclosed. We are withholding seventeen (17) pages in full. We are asserting FOIA subsection (b)(7)(E) as the justification for withholding.

A report titled *Certification Results High and Moderate Risks for TIGTA Enterprise Systems (TES)*, issued in 2013, consists of forty (40) pages. We are releasing to you one (1) page in full and two (2) pages in part. A copy is enclosed. We are withholding thirty-seven (37) pages in full. We are asserting FOIA subsections (b)(6), (b)(7)(C) and (b)(7)(E) as the justification for withholding

FOIA subsection (b)(6) permits the withholding of records and information about individuals when disclosure of the information could result in a clearly unwarranted invasion of personal privacy. The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. As a result, the privacy interests of the third parties outweigh the public's interest in having the information released.

FOIA subsection (b)(7)(C) permits an agency to withhold "information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy." The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. The information was compiled for law enforcement purposes and the privacy interest of the third parties outweighs the public's interest in having the information released. As a result, this information has been withheld in response to your request.

FOIA subsection (b)(7)(E) permits an agency to withhold "records or information compiled for law enforcement purposes ... [that] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could

reasonably be expected to risk circumvention of the law." The information withheld pursuant to this exemption was compiled in connection with an official review of TIGTA's programs or activities. The withheld information consists of techniques, guidelines or tolerances not known to the public and/or information that could lead to circumvention of the law. As a result, this information has been withheld in response to your request.

In reference to TD P 15-71, this is not a FOIA redaction. It is the removal of "Limited Official Use" or "Official Use Only" or "Sensitive But Unclassified" designation (and other legends) from TIGTA documents pursuant to Treasury Security Manual TD P 15-71.

In response to the second portion of your request regarding "potential attacks as well as audits and investigations conducted in the wake of a suspected or actual cyber attack, hacking incident or breach," TIGTA, as a bureau of the Department of the Treasury (Treasury), does not maintain this type of information; therefore, no records were located. TIGTA's information systems are hosted on the Treasury network.

Your request for a fee waiver is moot because no fees were assessed in the processing of your request.

If you have any questions, please contact Government Information Specialist Carroll Field at (202) 927-7032 or Carroll.Field@tigta.treas.gov and refer to Disclosure File # 2019-FOI-00166.

Alternatively, you may contact me, TIGTA's FOIA Public Liaison, at (202) 622-4068 or via email at Amy.Jones@tigta.treas.gov, for further assistance or to discuss any aspect of your request.

In addition, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration (NARA) to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, NARA, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Finally, if you are not satisfied with this determination in response to your request, you may administratively appeal this decision. We have enclosed an Information Sheet that explains the subsections cited above as well as your administrative appeal rights. Please address the envelope as follows:

Freedom of Information Act Appeal
Treasury Inspector General for Tax Administration
Office of Chief Counsel
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005

Also, you may electronically submit your appeal via Fax or E-mail:

FAX: 202-622-3339

E-MAIL: FOIA.Reading.Room@tigta.treas.gov

Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of this letter.

Sincerely,



Carroll Field
(For) Amy P. Jones
Disclosure Officer and
FOIA Public Liaison

Enclosures

Information on a TIGTA Determination to Withhold Records Exempt From the Freedom of Information Act – 5 U.S.C. § 552

Appeal Rights

You may file an appeal with the Treasury Inspector General for Tax Administration (TIGTA) within 90 days after we (1) determine to withhold records, (2) determine that no records exist, or (3) deny a fee waiver or a favorable fee category. If some records are released at a later date, you may file an appeal within 90 days from the date the last records were released. The appeal must be in writing, signed by you, and postmarked or electronically transmitted within 90 days from the date of the response letter. You must provide the following information: your name and address; description of the requested records; date of the initial request (and a copy, if possible); date of the letter denying the request (and a copy, if possible). You should mail your appeal to:

Freedom of Information Act Appeal
Treasury Inspector General for Tax Administration
Office of Chief Counsel
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005

Judicial Review

If we deny your appeal, or if we do not send you a reply within 20 days (not counting Saturdays, Sundays, or legal public holidays) after the date we receive the appeal, you may file a complaint with the U.S. District Court in the district where (1) you reside, (2) your principal place of business is located, or (3) the records are located. You may also file in the District Court for the District of Columbia.

Any proceedings in district court will be governed by the Federal Rules of Civil Procedure. Under Rule 4(i)(1) and (2), service on the Department of the Treasury may be effected by delivering copies of the summons and complaint: (a) personally, upon the U.S. Attorney (or his designee) for the district where the lawsuit is brought; (b) via registered or certified mail, upon the Attorney General of the United States at Washington, D.C.; and (c) via registered or certified mail to:

Treasury Inspector General for Tax Administration
Office of Chief Counsel
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005

In such a court case, the burden is on the Treasury Inspector General for Tax Administration to justify withholding the requested records, determining that no records exist, or denying a fee waiver or a favorable fee category. The court may assess against the United States reasonable attorney fees and other litigation costs incurred by the person who takes the case to court and who substantially prevails. You will have substantially prevailed if the court determines, among other factors, that you had to file the lawsuit to obtain the records you requested and that the Treasury Inspector General for Tax Administration had no reasonable grounds to withhold the records.

Exemptions

Not all records can be released under the FOIA. Congress established certain categories of information that are not required to be released in response to a FOIA request because release could be harmful to a government or private interest. These categories are called "exemptions" from disclosures. There are nine categories of exempt information and each is described below.

- (b)(1) (A) Specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b)(2) Related solely to the internal personnel rules and practices of an agency;

- (b)(3) Specifically exempted from disclosure by statute (other than section 552b of this title), if that statute--
 - (A) (i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or
 - (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and
 - (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.
- (b)(4) Trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) Inter-agency or intra-agency memorandums or letters which that would not be available by law to a party other than an agency in litigation with the agency, provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested;
- (b)(6) Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) Records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information:
 - (A) could reasonably be expected to interfere with enforcement proceedings,
 - (B) would deprive a person of a right to a fair trial or an impartial adjudication,
 - (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
 - (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,
 - (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or
 - (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) Contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) Geological and geophysical information and data, including maps, concerning wells.

Annual Assessment Report

Treasury Inspector General for Tax Administration (TIGTA)
Evaluation of TIGTA Enterprise System (TES) Controls
June 9, 2015



Contents

Overview	3
Detailed Findings.....	4

(b)(7)(E)



Overview

As documented in the Annual Assessment Authorization memo, dated April 10, 2015, the TIGTA Security and Compliance Services group recently conducted an assessment on TIGTA Enterprise System (TES) security controls. These controls are largely organization level and are applicable to all TIGTA systems and subsystems, including the Cybercrime Investigation System (CIS). This report documents the findings of that assessment.

(b)(7)(E)

The controls have been grouped by topic and functional area responsible for correcting the weaknesses. (b)(7)(E)

(b)(7)(E) Pursuant to Treasury policy, one of the following courses of action will be completed for each of the identified weaknesses within 60 days: remediate the weakness, create a plan of action and milestones (POA&M), or perform a risk assessment. The security group will work with the appropriate functional areas to identify which elements of the controls failed and, where applicable, generate closure statements, which are agreed upon conditions to be met in order to close the POA&M.

(b)(7)(E)

- (b)(7)(E)

-

(b)(7)(E)

**Certification Results
High and Moderate Risks
for
TIGTA Enterprise Systems (TES)**

Certification Results – High Moderate - TES

TD P 15-71

Table of Contents

1.0 Certification	3
2.0 Report.....	3

(b)(7)(E)



Certification Results – High Moderate - TES

TD P 15-71

1.0 Certification

As the Chief Information Security Officer (CISO), with the assistance of my team members, (b)(6)(b)(7)(C) (b)(6)(b)(7)(C), I have examined the TIGTA Enterprise System (TES) for compliance with Federal, Treasury, and TIGTA statutes, regulations, standards, and guidelines. I certify that the TES system has met or exceeded those requirements, except for the weaknesses stated in the TES risk assessment documents. Substantial portions of this risk assessment report were generated by a third party contractor, which was awarded by the Bureau of Public of Debt to help TIGTA to conduct an independent security test & evaluation for the TES system.

(b)(7)(E)

The TIGTA Security and Compliance Services group has been consistently involved in all Federal Information Security Management Act (FISMA) aspects for TES. This includes providing guidance on new technology implementations, participation in change control boards, policy development, security control implementation, and continuous monitoring.

(b)(7)(E)

2.0 Report

(b)(7)(E)

(b)(7)(E)